

Source-independent quantum random number generation via measuring coherence

Jiajun Ma, Xiao Yuan, Aishwarya Hakande, Xiongfeng Ma[†]

Center for Quantum Information, Institute for Interdisciplinary Information Sciences,
Tsinghua University, Beijing 100084, China

E-mail: [†]xma@tsinghua.edu.cn

Abstract. Measuring quantum states provides means to generate genuine random numbers. It has been shown that genuine randomness can be obtained even with an uncharacterized quantum source. In this work, we propose a framework that formalizes the idea of realizing source-independent quantum random number generation via measuring coherence. Without full state tomography, the coherence of the source can be estimated by coherence witnesses. The existing uncertainty-relation-based schemes can be treated as special cases under the coherence framework, as we design a nonlinear coherence witness that can essentially yield the same results. Meanwhile, we propose a source-independent random number generation scheme, which can achieve a higher randomness generation rate than the uncertainty-relation-based ones.

1. Introduction

Random number generation has many important applications in various tasks. In some cases, such as Monte Carlo simulation, it only requires the random numbers to be statistically unbiased. Pseudo random numbers or physical random numbers based on classical mechanics, such as coin flipping and noise measuring, are sufficient. The outcomes of these procedures may appear random, but they are in principle predictable. In cryptography, one of the security foundations lies on the unpredictability of random numbers, such as for the usage of keys. The random numbers via classical mechanic procedures are not suitable for cryptosystems. Therefore, it is important to study the generation of unpredictable (or genuine) random numbers.

According to Born's rule [1], the measurement outcome of a quantum system that is in the superposition of the measurement basis is unpredictable. Based on quantum mechanic principles, there are many quantum random number generation (QRNG) schemes proposed in the last two decades. For a review of the subject, one can refer to Ref. [2, 3] and the references therein. In general, a QRNG setup consists of two parts, a source that contains randomness and a measurement that readouts the randomness. As shown in Fig. 1, the source emits a sequence of quantum signals and the readout system measures them to produce random outcomes. For instance, if the states from the source are a sequence of qubits, $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and the measurement is a projection onto the $\{|0\rangle, |1\rangle\}$ basis, the outcomes are genuinely random.

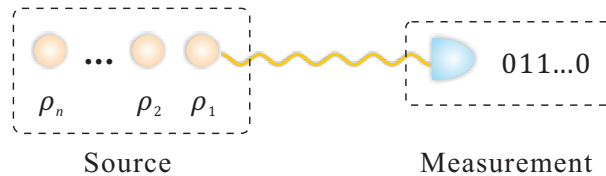


Figure 1: A quantum random number generator can be generally decomposed into two parts: source and measurement.

In practice, the source may contain both genuine randomness and classical noise. The latter can normally be influenced by some unexpected environment parameters, such as the temperature. In a cryptographic picture, an adversary, Eve, may take advantage of the classical noise. Consider a source that emits maximally mixed state $\rho = 1/2(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Although the measurement outcomes on the Z basis appear random, they are not genuinely random. This can be understood in the presence of Eve, who simply prepares $|0\rangle$ or $|1\rangle$ based on a predetermined random string. In this case, the measurement outcomes are entirely predictable. In fact, the bias in random number generators becomes a major security issues in current cryptosystems [4].

The key job of randomness analysis is to quantify the genuine randomness so that it can be extracted. One way of randomness quantification relies on modeling the QRNG implementation, which normally requires to calibrate the source and measurement devices [5]. In practice, however, the calibration is often hard to perform thoroughly.

Once implemented devices deviate from theoretical models, the randomness can be compromised. Several proposals have been proposed to solve this problem. For instance, QRNGs via certifying randomness based on nonlocality tests [6] are called self-testing or device-independent schemes, where neither the calibration of the quantum source nor the measurement is required. In practice, realizing a loophole free Bell test is experimentally challenging, which requires high-fidelity state preparation and detection efficiency, as well as the accurate chronological sequence control [7]. Furthermore, the randomness generation rate is quite limited owing to a small violation of Bell inequalities obtained with the state-of-the-art technology [8, 9].

In real-life applications, fully device-independent scenario may be too restrictive. By putting certain reasonable assumptions to devices, the performance of QRNGs would become practically acceptable. Along this direction, various efforts have been devoted to find a tradeoff between device independence and high randomness generation rate [10, 11, 12, 13]. In this paper, we focus on the scenario of generating genuine randomness with well-calibrated measurement devices but uncharacterized source, namely, source-independent quantum random number generation (SIQRNG) [11]. With certain reasonable assumptions on measurement devices, the SIQRNG schemes can be very practical. For instance, with a continuous-variable system, the randomness generation rate in such a scenario has achieved the Gbps regime [12]. The intuition behind these schemes is the quantum uncertainty relation. Given two complementary measurement bases, X and Z , if the outcome uncertainty of the X -basis measurement is small, its uncertainty of the Z -basis measurement must be large. The information on the complementary basis can be used to reveal the genuine randomness within the source. Since the uncertainty relation is state-independent, the QRNG schemes are source-independent.

Recently, genuine randomness has been shown to be essentially related to the coherence of the input quantum state in the measurement basis [14, 15]. There, the source is trusted and the extractable randomness is quantified in the asymptotic limit. In this paper, we propose a framework that extends this idea to a more general setting, where the source is uncharacterized and the measurement outcomes are finite. We show that SIQRNG can be realized via measuring coherence of the input quantum state. Moreover, we propose a method of estimating the coherence via coherence witnesses. By designing a nonlinear coherence witness, we show that the coherence estimation yields the same randomness quantification with the previous uncertainty-relation-based SIQRNG schemes. Furthermore, we propose a SIQRNG scheme that generally enjoys a higher randomness generation rate than the uncertainty-relation-based ones.

The paper is organized as follows. In Sec. 2, we review the preliminaries on coherence measures and SIQRNG. Then, in Sec. 3, we introduce a witness to measure the coherence. In Sec. 4, we present the framework of QRNG via measuring coherence, based on which, a SIQRNG protocol is proposed in Sec. 5. In Sec. 6, with numerical simulations, we show that our protocol generally enjoys a higher randomness generation rate than the uncertainty-relation-based schemes. Finally, we conclude in Sec. 7.

2. Preliminaries: Coherence and SIQRNG

2.1. Resource theory of coherence

The resource theory of coherence formalizes the intuition that quantum superpositions are non-classical [16]. In this framework, with an orthogonal basis, $\Pi = \{|i\rangle\}$, as the reference basis, one can define the free state (incoherent state) as $\sigma = \sum_i p_i |i\rangle \langle i|$, with $\{p_i\} \geq 0$ and $\sum_i p_i = 1$. The free operations (incoherent operations) are the set of operations that take incoherent states to incoherent states. Specifically, they are formed by the Kraus operators, $\{K_i\}$, that satisfy $K_i \mathcal{I} K_i^\dagger \in \mathcal{I}$, where \mathcal{I} is the set of incoherent states.

Under this resource framework, a coherence measure needs to fulfill a few criteria. There are many proposals for coherence measures, such as the l_1 -norm of coherence [16], the coherence of formation [14], and the robustness of coherence [17]. In this paper, we adopt the relative entropy of coherence [16],

$$C(\rho) = H(\Delta_\Pi(\rho)) - H(\rho), \quad (2.1)$$

where $H(\rho)$ is the von Neumann entropy of ρ and $\Delta_\Pi(\rho) \equiv \sum_i |i\rangle \langle i| \rho |i\rangle \langle i|$ is the dephasing operation in the reference basis Π . Recently, the relative entropy of coherence is linked to the genuine randomness obtained by measuring ρ in the basis Π [15].

2.2. SIQRNG

In the framework of SIQRNG, illustrated in Fig. 2, Eve prepares a sequence of quantum states represented by τ_{AE} . Then she sends the subsystem A to the legitimate user, Alice, and retains the rest E . Alice divides the received state $\tau_A = \text{Tr}_E(\tau_{AE})$ into N partition states and measures each state in some basis. Alice tries to extract genuine randomness from the measurement outcome. Meanwhile, Eve aims at predicting the random numbers extracted from τ_A with the assistance of τ_E .

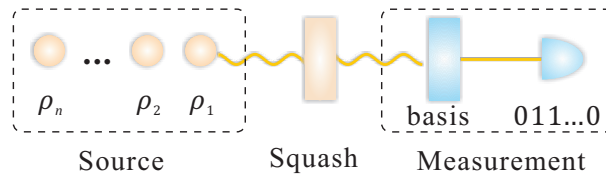


Figure 2: Source independent quantum random number generator. The squashing model transfers the input states into qubits. Based on additional random inputs, the readout system randomly choose a basis to measure the received state.

Since the source is untrusted and uncharacterized, τ_A can be prepared in an arbitrary dimensional Hilbert space. On the other hand, Alice's outcome is either 0 or 1, which implies her measurement resembles a qubit measurement. One can think of Alice projecting the received state to a qubit first and then performing measurement.

This projection is called squashing operation [18, 19]. The challenge lies on proving the equivalence between a practical measurement and squashing operation plus a qubit measurement with an arbitrary state input. Fortunately, the squashing model has been proven to be satisfied in the common optical implementations using threshold detectors with proper postprocessing [20, 21].

After the squashing operation, Alice can project the state τ_A to n qubits and $N - n$ vacuum states. Alice performs qubit measurements on the n qubits. The rest $N - n$ vacuum states can be regarded as measurement losses. Since measurement devices are trusted in the SIQRNG scenario, one can assume that the n qubits are fair-sampled from the N states. That is, here the detection efficiency loophole is not considered. The following randomness analysis will focus on the n squashed qubits.

Here, we briefly review the previous SIQRNG scheme [11].

- 1) An untrusted source (controlled by Eve) emits a sequence of quantum states.
- 2) Alice (or Eve) squashes the quantum states into qubits and vacua. Alice discards the vacua and retains the n squashed qubits.
- 3) Alice randomly chooses n_x qubits out of the n squashed qubits and measures them in the X basis. Within n_x outcomes, the ratio of outcome $|-\rangle$ is e_{xb} , which is defined to be the error rate. Ideally, Alice expects the source to emit the state $|+\rangle$ and hence the result of $|-\rangle$ is defined as an error.
- 4) Alice measures the rest $n_z = n - n_x$ squashed qubits in the Z basis to obtain n_z raw random bits.
- 5) Alice extracts $n_z(1 - S(e_{xb} + \theta)) - t_e$ random bits from the raw random bits using a universal hashing function, where S is the binary Shannon entropy, θ is the statistical deviation parameter and 2^{-t_e} is the failure probability of the randomness extraction.

In above scheme, the security proof techniques of quantum key distribution (QKD) are employed in the randomness analysis. Here is the argument. Ideally, the source should emit states $|+\rangle$. Then, Alice measures them in the Z basis, $\{|0\rangle, |1\rangle\}$, to generate random numbers. In scenario of SIQRNG, the source is allowed to emit arbitrary quantum states in arbitrary dimensions. On the measurement end, one can consider a virtual protocol. First, a squashing model is applied to project the quantum states into a sequence of qubit and vacuum states. Then Alice performs an error correction procedure that transforms all states to $|+\rangle$. Finally she measures them in the Z basis. By designing the error correcting code appropriately, this operation can be commute with the Z -basis measurement [22]. Also the squashing model is proven to be equivalent to the threshold detection model with appropriate postprocessing [20]. Hence, Alice does not need to perform the virtual protocol, which requires a universal quantum computer. Instead, she can perform the Z -basis measurement first and then apply a randomness extraction on the measurement outcomes. The latter essentially functions the same as the error correction procedure in the virtual protocol.

In the randomness extraction, or the error correction in the virtual protocol, Alice needs to know the error rate in the X basis, $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Thus, in the SIQRNG scheme, Alice needs to randomly test the quantum state in the X basis to estimate its error rate, which is later used for randomness quantification [11].

In this paper, we would show the randomness of SIQRNG from a difference perspective. The idea is based on the recently discovered link between coherence and genuine randomness in a quantum state [14, 15]. Instead of applying error correction, Alice estimates the coherence of the qubit states via measuring randomly sampled qubit states. Then she measures the rest qubits in the Z basis to generate the raw randomness. The estimated coherence are used to bound the genuine randomness of the raw data. In postprocessing, she distills the genuine randomness from the raw data.

3. Measuring coherence with coherence witness

Normally, to estimate the coherence of an unknown state, one needs to perform a full state tomography to obtain the density matrix ρ . In some cases, full tomography information is not available. For example, as the dimension of the state increases, the number of required measurement in tomography increases quadratically, which becomes very challenging for experiments. Thus, it is interesting to estimate the coherence of an unknown state without a full tomography.

A similar problem raises in the field of entanglement measure, where it is expected to estimate the entanglement with a limited number of measurements. The solution there is to employ entanglement witnesses, which are originally designed to justify whether quantum states are entangled or not, to estimate entanglement [23, 24]. Recently, this idea has been extended to the resource theory of coherence [17], i.e., estimating the coherence with coherence witnesses.

The original coherence witness is a linear function of the density matrix ρ [17]. Here, we extend this notion to an arbitrary function of ρ .

Definition 1. A coherence witness is a function of ρ , $W(\rho)$, that satisfies the following criteria,

- (i) $\forall \rho \in \mathcal{I}, W(\rho) \geq 0$;
- (ii) $\exists \rho \notin \mathcal{I}, W(\rho) < 0$.

A linear coherence witness has been shown to be useful to bound the coherence [17]. Here, we design a nonlinear coherence witness to bound the relative entropy of coherence.

Lemma 1. Given a reference basis $\Pi = \{|i\rangle\}$ in a d -dimensional Hilbert space,

$$W_u(\rho) = H(\Delta_\Xi(\rho)) - \log_2 d, \quad (3.1)$$

is an coherence witness, where Ξ is a mutually unbiased basis of Π .

Proof. It is not hard to see that $\forall \rho \in \mathcal{I}$, one has $W_u(\rho) = 0$, since Ξ is a mutually unbiased basis of Π . Also, for $\rho = |i'\rangle\langle i'|$ where $|i'\rangle \in \Xi$, $W_u(\rho) = -\log_2 d < 0$. \square

Theorem 1. *Given a reference basis $\Pi = \{|i\rangle\}$ and a state ρ in a d -dimensional Hilbert space, the relative entropy of coherence, $C(\rho)$, can be bounded by the coherence witness $W_u(\rho)$ defined in Eq. (3.1),*

$$C(\rho) \geq -W_u(\rho) = \log_2 d - H(\Delta_\Xi(\rho)), \quad (3.2)$$

where Ξ is a mutually unbiased basis of Π .

Proof. The dephasing operators, $\Delta_\Pi(\rho)$ and $\Delta_\Xi(\rho)$, can be viewed as two projection measurements, which have the quantum uncertainty relation [25],

$$H(\Delta_\Pi(\rho)) + H(\Delta_\Xi(\rho)) \geq -\log_2 c + H(\rho), \quad (3.3)$$

where $c = \max_{i,i'} |\langle i|i'\rangle|^2$, with $|i\rangle \in \Pi$ and $|i'\rangle \in \Xi$.

The two bases Π and Ξ are mutually unbiased, and hence $c = 1/d$. Rearranging the terms in Eq.(3.3) and using the definition $C(\rho) = H(\Delta_\Pi(\rho)) - H(\rho)$, Eq.(3.2) is obtained. □

From Theorem 1, one can estimate the relative entropy of coherence via measuring the state in the complementary basis of the reference basis. This idea is similar to the one employed in the uncertainty-relation-based SIQRNG [11, 12]. There, the intrinsic randomness generated via the Z -basis measurement is estimated by measuring the state in the complementary X basis. In the next section, we propose a framework that formalizes the relation between these two scenarios.

4. Framework of SIQRNG via measuring coherence

The task of estimating coherence of an unknown quantum state shares similarities with randomness evaluation in SIQRNG. In both scenarios, the source state is uncharacterized while the measurement is trusted. Meanwhile, the amount of genuine randomness within the source can be quantified by the coherence of the quantum state [14, 15]. Therefore, extracting genuine randomness in SIQRNG can be reduced to the problem of estimating coherence within the source. In this section, we would present an framework that links the two tasks.

4.1. Quantification of randomness

Following the discussion of SIQRNG in Sec. 2, we focus on the n squashed qubits, which contribute one raw data bit each. Alice needs to quantify the genuine randomness in the n -bit raw data from the n -qubit state, $\tau_A = \text{Tr}_E(\tau_{AE}) \in \mathcal{H}_2^{\otimes n}$, where \mathcal{H}_2 denotes a two-dimensional Hilbert space. In the partial trace, we put the $N - n$ vacuum states to system E . Note that the n qubits can be correlated with each other, or even with Eve's system τ_E .

Suppose Alice randomly chooses n_z qubits and measures them in the Z basis to generate raw random bits, while she measures the rest $n - n_z$ qubits in some other

complementary bases for parameter estimation, which would give Alice information about τ_A . Denote the measurement outcome in the Z basis (an n_z -bit string) by K_z . Here, Alice's measurement can be viewed as a dephasing operation on each qubit of subsystem A in the Z basis, $\Delta_{Z^{\otimes n_z}}^A(\tau_{AE})$. Then the randomness contained in K_z is quantified by [26],

$$R^{\varepsilon_1}(K_z) = \min_{\tau_{AE}} H_{\min}^{\varepsilon_1}(A|E)_{\Delta_{Z^{\otimes n_z}}^A(\tau_{AE})}, \quad (4.1)$$

where the minimization runs over all possible states of Eve that satisfy $\text{Tr}_E(\tau_{AE}) = \tau_A$, and $H_{\min}^{\varepsilon_1}$ is the smooth min-entropy, defined in Appendix A, with a smooth parameter ε_1 .

The min-entropy $R^{\varepsilon_1}(K_z)$ is the key parameter for randomness extraction. With universal hashing [27], such as Teoplitz-matrix hashing, one can extract random bits that are ε -close to a uniformly distributed string from Eve's point of view. Here, the security parameter is $\varepsilon = \varepsilon_1 + \varepsilon_2$, with ε_2 the failure probability introduced in the randomness extraction procedure.

4.2. Randomness analysis

In the following, we analyze the randomness with the assumption that the n squashed qubits are independent and identically distributed (i.i.d.). This assumption is also made in the scenario of collective attacks in QKD, where Eve attacks each signal in an i.i.d. manner. In a more general setting, the n qubits might be entangled, which corresponds to the scenario of coherent attacks in QKD. It is proven that the security parameter for coherent attacks is only polynomially larger than the security parameter for collective attacks [28]. The extra information available to the adversary for coherent attacks can be compensated by slightly reducing the size of the final random bits in the privacy amplification stage. We expect that a similar argument can be employed here to obtain the security proof against the most general sources. We leave the randomness analysis with an correlated source for future study.

With the i.i.d. assumption, the joint state that outputs the raw random bits can be expressed by $\tau_{AE} = \rho_{AE}^{\otimes n_z}$. From Eq. (4.1), one can have

$$R^{\varepsilon_1}(K_z) = \min_{\rho_{AE}} H_{\min}^{\varepsilon_1}(A|E)_{\Delta_{Z^{\otimes n_z}}^A(\rho_{AE}^{\otimes n_z})}. \quad (4.2)$$

For $n_z \geq \frac{8}{5} \log_2 \frac{2}{\varepsilon_1^2}$, the smooth min-entropy can be lower bounded by the conditional von Neumann entropy, defined as $H(A|E)_{\rho_{AE}} = H(\rho_{AE}) - H(\rho_E)$ [29]. Thus one has

$$R^{\varepsilon_1}(K_z) \geq n_z \min_{\rho_{AE}} H(A|E)_{\Delta_Z^A(\rho_{AE})} - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}, \quad (4.3)$$

whose derivation is shown in Appendix B. Meanwhile, $\min_{\rho_{AE}} H(A|E)_{\Delta_Z^A(\rho_{AE})}$ is related to the relative entropy of coherence of ρ_A [15],

$$\min_{\rho_{AE}} H(A|E)_{\Delta_Z^A(\rho_{AE})} = C(\rho_A), \quad (4.4)$$

where the reference basis for $C(\rho_A)$ is the Z basis. Inserting Eq. (4.4) into Eq. (4.3), one has

$$R^{\varepsilon_1}(K_z) \geq n_z C(\rho_A) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}. \quad (4.5)$$

We remark that this expression only holds for $n_z \geq \frac{8}{5} \log_2 \frac{2}{\varepsilon_1^2}$, which is normally satisfied in practice, typically, $n_z \geq 95$ for $\varepsilon_1 = 10^{-10}$.

4.3. Randomness analysis via coherence witness

The randomness analysis result, Eq. (4.5), implies that one can estimate the amount of randomness in a quantum state by measuring the coherence of the state. In Sec. 3, we have shown that, without a full state tomography, one can lower bound the coherence with coherence witnesses. Therefore, there is a close relation between coherence witness and SIQRNG: any coherence witness that is able to lower bound the coherence can be employed to realize a SIQRNG scheme.

As an example, we apply this analysis method to the SIQRNG scheme described in Sec. 2.2. The measurement used by Alice in the SIQRNG scheme forms a coherence witness, W_u , as shown in Eq. (3.1). Then, applying Theorem 1 to Eq. (4.5), the number of genuine random bits, denoted by $R_u^{\varepsilon_1}$, is estimated by

$$R_u^{\varepsilon_1} \geq -n_z W_u(\rho_A) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}, \quad (4.6)$$

where $W_u(\rho_A) = H(\Delta_X(\rho_A)) - 1$. In the asymptotic limit, when the number of emitted qubits n approaches infinitely large, the randomness generation rate is given by

$$r_u = \frac{R_u^{\varepsilon_1}}{N} \big|_{N \rightarrow \infty} \geq q\beta(1 - H(\Delta_X(\rho_A))), \quad (4.7)$$

where $\beta = n/N$ is the transmittance of the signal, and $q = n_z/n$ is the ratio of Z -basis measurement. In this limit, Alice can set $q \rightarrow 1$ to maximize r_u . Note that Eq. (4.7) coincides with the randomness generation rate evaluated via the complementary uncertainty relation [11].

5. Tomography-based SIQRNG

Note that the SIQRNG protocols based on the complementary uncertainty relation do not necessarily extract the maximal amount of the randomness from the source. For instance, suppose that the source emits state $(|0\rangle + i|1\rangle)/\sqrt{2}$, from Eq. (4.7), one obtain a lower bound of r_u to be 0, thus no genuine randomness can be extracted. Nevertheless, the measurement outcome on the Z basis is in fact genuinely random. In this case, the genuine randomness cannot be revealed by the coherence witness using the X measurement. Instead, the randomness can be witnessed with another complementary basis $Y = \{|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}\}$. Without a priori knowledge of the source, one might choose a bad witness to underestimate the genuine randomness.

For the SIQRNG scheme described in Sec. 2.2, by adding one more measurement basis, Alice can obtain a better estimation of the coherence of ρ_A via a full state tomography. Then she can extract more genuine randomness from the raw data. Based on this observation, we propose a SIQRNG protocol based on tomography, as presented in Table 1.

Table 1: Source-independent quantum random number generation

1. State preparation:

- (a) An untrusted source (might be controlled by Eve) emits N quantum states in arbitrary dimensions, which are sequentially sent to the readout system.
- (b) An *squashing operation* transforms the quantum states into n qubits and $N - n$ vacua.

2. Measurement:

- (a) The $N - n$ vacua are discarded and the remaining n squashed qubit states are post-selected for randomness generation.
- (b) Alice randomly chooses n_x , n_y , and n_z qubits for the X -, Y -, and Z -basis measurements, with probability $q_x = q$, $q_y = q$, $q_z = 1 - 2q$, respectively. Denote p_x , p_y , and p_z to be the rates to obtain the outcomes $|+\rangle$, $|i+\rangle$, and $|0\rangle$, respectively.
- (c) The Z -basis measurement outcomes are recorded as the raw data.

3. State tomography: with the measurement results, p_x , p_y , and p_z , Alice can estimate the density matrix of the squashed qubits, ρ_A . Note that statistical fluctuations need to be considered here.

4. Randomness evaluation and extraction: with the information of ρ_A , Alice can bound the genuine randomness of the raw data and apply a proper randomness extractor to obtain the final random bits.

In the protocol, the coherence of the source $C(\rho_A)$ can be accurately estimated with a full tomography of ρ_A . Then, the number of genuine random bits, denoted by $R_t^{\varepsilon_1}$, can be estimated via Eq. (4.5),

$$R_t^{\varepsilon_1} \geq n_z C(\rho_A) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}. \quad (5.1)$$

In the asymptotic limit, the randomness generation rate, denoted by r_t , is given by

$$r_t \geq \frac{R_t^{\varepsilon_1}}{N} \Big|_{N \rightarrow \infty} = q_z \beta C(\rho_A), \quad (5.2)$$

where $\beta = n/N$ is the transmittance of the signal and $q_z = n_z/n$ is the ratio of Z -basis measurement. In large data-size limit, Alice can set $q_z \rightarrow 1$.

In tomography, the density matrix, ρ_A can be estimated from measurement outcomes, p_x , p_y , and p_z , defined in Table 1. Write ρ_A as $\rho_A = (I + (2\vec{p} - 1) \cdot \vec{\sigma})/2$, where $\vec{p} = (p_x, p_y, p_z)$ and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices. Substituting ρ_A into Eq. (2.1) and (5.1), one can get

$$C(\rho_A) = H(p_z) - H\left(\frac{p_o + 1}{2}\right), \quad (5.3)$$

$$R_t^{\varepsilon_1} \geq n_z H(p_z) - n_z H\left(\frac{p_o + 1}{2}\right) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}, \quad (5.4)$$

where $p_o = \sqrt{4(p_x^2 + p_y^2 + p_z^2 - p_x - p_y - p_z) + 3}$.

5.1. Squashing model

As discussed in Sec. 2, the squashing model should be applied to project the quantum state from the uncharacterized source into a sequence of qubits. The squashing model requires that, depending on the measurement setting, appropriate postprocessing should be implemented. Here, Alice can employ the postprocessing of squashing model used in the analysis of quantum state tomography [21].

According to the Supplementary Materials of Ref. [21], the double click events should be considered to derive a set of bounds of the obtained statistics. Specifically, for each measurement bases $j \in \{X, Y, Z\}$, let n_j^0 , n_j^1 and n_j^d denote the numbers of the two single-click events and the double-click event, respectively. Then Alice obtains a set of qubit states, \mathcal{S} , that are compatible with the measurement results. That is, they fulfill the following constraints,

$$\frac{n_j^0}{n_j^0 + n_j^1 + n_j^d} \leq p_j \leq \frac{n_j^0 + n_j^d}{n_j^0 + n_j^1 + n_j^d}. \quad (5.5)$$

In the following, we denote the lower bound for p_j in above inequalities by p_j^L , and the upper bound by p_j^U .

In our protocol, Alice needs to consider the worst case of $\rho_A \in \mathcal{S}$. That is, she should minimize $C(\rho_A)$ in Eq.(5.3) over \mathcal{S} . In Appendix C, we show that $C(\rho_A)$ is a unimodal function with respect to each p_j , with the minimal value achieved for $p_j = 1/2$. Without loss of generality, from now on, we assume $p_j^U \geq 1/2$, otherwise Alice can flip the bit label in the j basis. Denote the worst case value of p_j for the coherence quantification by p_j^w , thus $p_j^w = \max(p_j^L, 1/2)$.

5.2. Double clicks

As discussed in Sec. 5.1, it is possible to have double-click events in measurement, which should be taken into account in the tomography testing step. In addition, as the measurement outcome in the Z basis is also used to generate the raw random bits, one should implement some postprocessing on these data to map them to single-value outcomes. Note that the double-click events in the X and Y bases do not need this

postprocessing, since they are only used for tomography testing in Eq. (5.5) where Alice only needs to count the number of double clicks. As will shown later, this postprocessing, such as random assignment, generally consumes randomness, which should be taken into account when evaluating the net randomness generation rate.

5.2.1. Random assignment method Here, we consider a postprocessing method that Alice randomly assigns 0 or 1 for the double-click events in the Z basis. After the squashing model analysis, Alice obtains p_z^w as the worst case estimation of p_z . Then, in the random assignment procedure, the probability of assigning value 0 to the double-click events, denoted by p_a , should be compatible with p_z^w ,

$$p_z^w = \frac{n_z^0 + p_a n_z^d}{n_z^0 + n_z^1 + n_z^d}. \quad (5.6)$$

Thus, p_a is given by

$$p_a = \frac{p_z^w n_z - n_z^0}{n_z^d}. \quad (5.7)$$

The randomness cost in the double-click assignment procedure is $n_z^d H(p_a)$. Thus the net randomness generation rate is given by,

$$\begin{aligned} R_t^n &= R_t^{\varepsilon_1} - n_z^d H(p_a) \\ &\geq n_z H(p_z^w) - n_z H\left(\frac{p_z^w + 1}{2}\right) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}} - n_z^d H(p_a), \end{aligned} \quad (5.8)$$

where $p_o^w = \sqrt{4(p_x^{w2} + p_y^{w2} + p_z^{w2} - p_x^w - p_y^w - p_z^w) + 3}$

5.2.2. Discard method In practice, the random assignment might be technically challenging to implement. Thus, we consider an easier method to deal with the double-click events in the Z basis — discarding all the double-click events. Let ρ^s and ρ^d denote the density matrix after squashing model that correspond to the single-click events and the double-click events, respectively. Then, one has $p_d \rho_A^d + (1 - p_d) \rho_A^s = \rho_A$, where $p_d = n_z^d / n_z$ is the ratio of double-click events in the Z basis. Once discarding all the double-click events, the random bits in the remaining data can be lower bounded by

$$R_t^n \geq n_z^s C(\rho_A^s) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}, \quad (5.9)$$

where $n_z^s = n_z - n_z^d$ is the number of single-click events in the Z basis. To estimate $C(\rho_A^s)$, one can employ the concavity of relative entropy of coherence,

$$p_d C(\rho_A^d) + (1 - p_d) C(\rho_A^s) \geq C(\rho_A). \quad (5.10)$$

Thus

$$\begin{aligned} n_z^s C(\rho_A^s) &\geq n_z C(\rho_A) - n_d C(\rho_A^d) \\ &\geq n_z C(\rho_A) - n_d. \end{aligned} \quad (5.11)$$

where $C(\rho_A^d) \leq 1$ is used in the second inequality. Combining Eq. (5.11), (5.9), and (5.3), the net randomness generation rate is given by

$$R_t^n \geq n_z H(p_z^w) - n_z H\left(\frac{p_o^w + 1}{2}\right) - 7.09 \sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}} - n_z^d \quad (5.12)$$

Note that the randomness generation rate by the discard method is generally smaller than that by the random assignment method in Eq. (5.8).

5.3. Analysis of statistic fluctuations

In practice, the number of squashed qubits n is finite. Thus the probabilities used for parameter estimation would suffer from statistical fluctuations. Here, we analyze the finite-data-size effect on the estimation of p_j^w . In order to distinguish the probabilities with the measurement rates, denote the expectation values of p_j^w to be \bar{p}_j , which would be inserted into Eq. (5.4) to evaluate the genuine randomness. Since the qubits are assumed to be i.i.d., Alice can employ the Hoeffding inequality [30] to estimate the discrepancy between p_j^w and \bar{p}_j caused by the statistical fluctuations,

$$\text{Prob}(\bar{p}_j \leq p_j^w - \theta) \leq e^{-2\theta^2 n_j} = \varepsilon_j, \quad (5.13)$$

Here, we assume $p_j^w - \theta \geq 1/2$, otherwise we take the worst bound $\bar{p}_j = 1/2$. Replacing $\{p_j^w\}$ by $\{p_j^w - \theta\}$ in Eq. (5.8) or (5.12), one can obtain the lower bound of randomness with a total failure probability,

$$\varepsilon = \varepsilon_1 + \varepsilon_2 + \varepsilon_x + \varepsilon_y + \varepsilon_z, \quad (5.14)$$

where ε_1 is introduced by the smooth parameter and ε_2 is introduced by randomness extraction.

6. Simulation

In this section, we first analyze the performance of the tomography-based SIQRNG and compare it to the original proposal. Then, by taking account of statistical fluctuations, we optimize the ratio of qubits used for the tomography testing.

6.1. Comparing to the original SIQRNG

For simplicity, we consider the asymptotic limit where the number of emitted quantum states N is infinitely large. Then, the randomness generation rate for the original protocol is given by Eq. (4.7), while the rate for the tomography-based protocol is given by Eq. (5.2). In both cases, q_z is set to be 1. Besides, we assume the single photon source is used without considering the photon loss and the detector inefficiency, and hence the transmittance $\beta = 1$. Then, the randomness generation rate for the original protocol is given by

$$r_u|_{q_z=1, \beta=1} \geq 1 - H(\Delta_X(\rho_A)), \quad (6.1)$$

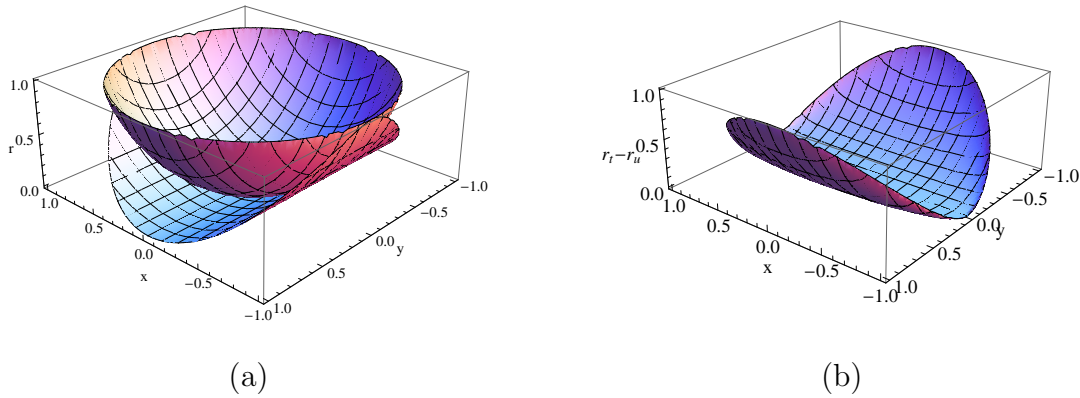


Figure 3: Comparison of the randomness generation rates with an input qubit state $\rho_A = \frac{I+x\sigma_x+y\sigma_y}{2}$, with $N \rightarrow \infty, q_z = 1, \beta = 1$. (a) The lower surface describes the randomness generation rate for the uncertainty-relation-based scheme r_u as shown in Eq. (6.1), while the upper surface describes the randomness generation rate for the tomography based scheme r_t as shown in Eq. (6.2). (b) Illustration of the gap between the two schemes, $r_t - r_u \geq 0$.

and the tomography-based protocol by

$$r_t|_{q_z=1, \beta=1} \geq C(\rho_A). \quad (6.2)$$

In the comparison, we assume the input state has the form of $\rho_A = (I+x\sigma_x+y\sigma_y)/2$, where x and y are two parameters and $x^2 + y^2 \leq 1$. The comparison between Eq. (6.1) and (6.2) is illustrated in Fig. 3. One can clearly see that the tomography-based scheme generally provides a higher randomness generation rate than the original proposal. The larger the parameter y is, the bigger gap the two schemes has. In general, one can consider a more general state, $\rho_A = (I+x\sigma_x+y\sigma_y+z\sigma_z)/2$, where the gap of randomness generation rate between the two schemes is nonzero as long as $y \neq 0$.

6.2. Parameter optimization

Now we analyze the performance of the tomography-based protocol by simulating a practical experiment setup. Details of the simulation model is presented in Appendix D. Consider a practical source, consisting of a laser and a polarization modulator, which emits N coherent-state pulses with an intensity of μ_0 . We assume the quantum state is prepared to be $|+\rangle$, which is then transmitted through a depolarization channel. Thus, the received quantum state can be described by

$$\rho_A = p\frac{I}{2} + (1-p)|+\rangle\langle+|, \quad (6.3)$$

where $p \in [0, 1]$. The readout system consists of a polarization rotator (used for basis selection), a polarization beam splitter, and two threshold detectors with the same detection efficiencies. Denote the total transmittance by η , including the detector efficiency and the coupling efficiency between the source and the detector. It is

equivalent to consider a coherent state with intensity of $\mu \equiv \mu_0\eta$. Here, we ignore the detection caused by dark count since for QRNG, dark counts are normally negligible comparing to η . For a more comprehensive model taking account of dark counts, one can refer to the corresponding QKD model [31].

In this model, we put the misalignment errors into the parameter p . Then, the simulated worst estimations of p_j are given by,

$$\bar{p}_x = \frac{1 - p - e^{-\mu} + pe^{-\frac{\mu}{2}}}{1 - e^{-\mu}} - \theta, \quad (6.4)$$

$$\bar{p}_y = \frac{e^{-\frac{\mu}{2}} - e^{-\mu}}{1 - e^{-\mu}} - \theta, \quad (6.5)$$

$$\bar{p}_z = \frac{e^{-\frac{\mu}{2}} - e^{-\mu}}{1 - e^{-\mu}} - \theta. \quad (6.6)$$

Meanwhile, the number of double click events in the Z basis is

$$n_z^d = N(1 - 2q)(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}). \quad (6.7)$$

The detailed model with the calculations of Eq. (6.4) - (6.7) are shown in Appendix D. Note that all the \bar{p}_j here are less than $1/2$, as required in the randomness analysis shown in Sec. 5. Then one can evaluate the extractable randomness from Eq. (5.12)[‡].

In the simulation, we pick $p = 0$, $p = 0.1$, $p = 0.3$ for the input state of Eq. (6.3), and set $\varepsilon_x = \varepsilon_y = \varepsilon_z = \varepsilon_1 = \varepsilon_2 = 10^{-10}$ and the number of pulses $N = 10^{10}$. First, by optimizing the tomography testing parameter q , we show the dependence of the randomness generation rate, given by Eq. (5.12), on the intensity μ in Fig. 4. From the figure, one can see that initially, the randomness generation rate increases with the intensity of the signal μ , due to the increase of the single-click events relative to the no-click events. As μ keeps increasing, the double-click events become dominant. Then, the randomness generation rate starts to decreases. Thus, there is an optimal choice of μ . In experiment, one should characterize total transmittance η first and then set the light intensity μ_0 to make $\mu = \mu_0\eta$ optimal.

Next, we investigate how the optimal tomography testing parameter, q , varies with the number of pulses, N . Here, we pick $p = 0.1$ and optimize the the intensity μ . When $N \leq 10^{4.8}$, no net random bits can be generated. One can see from Fig. 5(a) that the optimal q starts from 0.14 and drops down close to 0 with the increase of N . This is consistent with the intuition that $q_z = 1 - 2q \rightarrow 1$ as N goes to infinite. Note that the optimization of q assume that $q_x = q_y$ in the tomography-based protocol. In general, one can optimize q_x and q_y separately.

We also investigate how the randomness generate rate varies with the number of pulses N , as shown in Fig. 5(b). Here, we pick $p = 0.1$ and optimize both the intensity μ and the tomography testing parameter q . One can see that no randomness can be obtained as $N \leq 10^{4.8}$, beyond which point the rate increases with N . This increase is

[‡] Here, we adopt the discard method to process the double-click events in the Z basis. In fact, one would obtain the same randomness generate rate by the random assignment method in the case of Eq. (6.3).

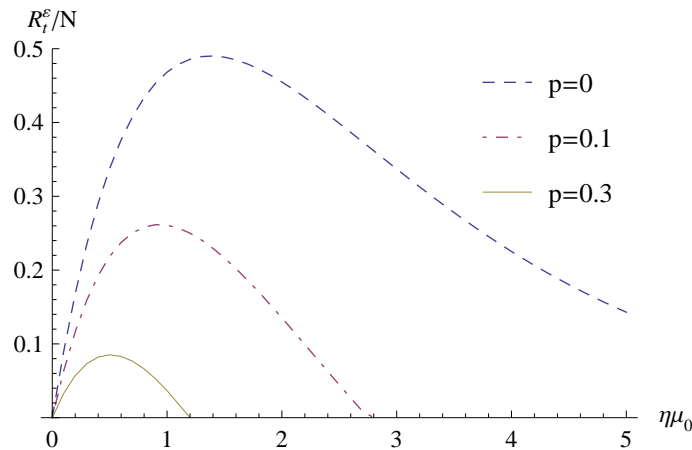


Figure 4: Randomness generation rate vs. intensity μ with various depolarization parameters p . The optimal μ for $p = 0, 0.1, 0.3$ are $\mu = 1.4, 0.9, 0.5$, respectively.

mainly contributed by the increase ratio of Z -basis measurement as N becomes large. This is similar to the biased basis case in QKD [32].

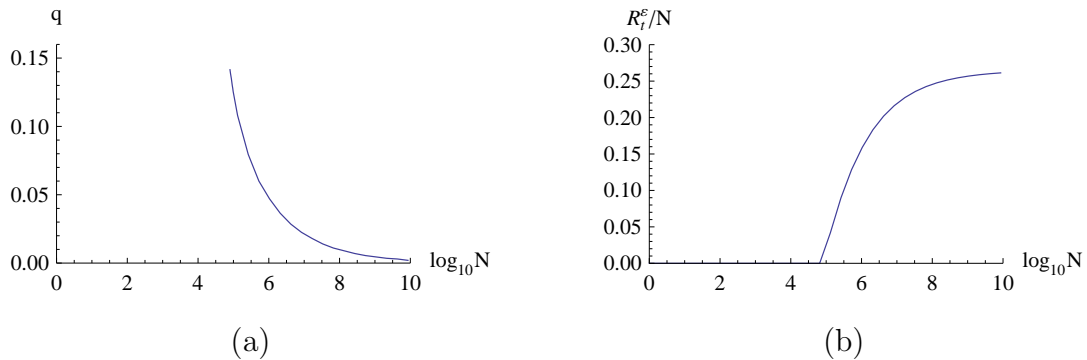


Figure 5: The performance of the tomography based SIQRNG by optimizing the basis selection parameter q , where we pick $p = 0.1$ and have the intensity parameter μ optimized. (a) shows the optimal value of q versus the number of the pulses N . (b) illustrates the randomness generate rate $R_i^ε/N$ versus the number of the pulses N .

7. Discussion

In this paper, we propose a framework that realize the SIQRNG with measuring coherence of an unknown quantum state. We show that the uncertainty-relation-based SIQRNG is essentially related to estimating the relative entropy of coherence with a coherence witness. Furthermore, we propose a SIQRNG scheme based on state tomography and take account of the statistical fluctuations. By simulating the QRNG,

we show that our protocol generally enjoys a higher randomness generation rate than the uncertainty-relation-based ones.

Along this direction, one can realize a SIQRNG scheme by designing the coherence witness that is adapted to specific experimental conditions. Besides, it is promising to extend the framework to high-dimensional QRNG, e.g., schemes based on continuous variables [12] or laser phase fluctuations [33]. A possible challenge of this extension is the development of the high-dimensional squashing model.

Acknowledgments

We thank Zhen Zhang for fruitful discussions. This work was supported by the National Natural Science Foundation of China Grant No. 11674193.

Appendix A. Smooth min-entropy

In this section, we provide the definition of smooth min-entropy [26].

Definition 2. *Given a bipartite density operator ρ_{AE} , the min-entropy of A conditioned on E is defined as*

$$H_{\min}(A|E)_{\rho_{AE}} \equiv -\min_{\sigma_E} D_{\infty}(\rho_{AE} || \mathbb{I} \otimes \sigma_E) \quad (\text{A.1})$$

where the minimization ranges over all normalized density operators σ_E on E and

$$D_{\infty}(\tau || \tau') \equiv \min\{\lambda \in \mathbb{R} : \tau \leq 2^{\lambda} \tau'\}. \quad (\text{A.2})$$

Then the smooth min-entropy of A conditioned on E is defined as

$$H_{\min}^{\varepsilon}(A|E)_{\rho_{AE}} \equiv \sup_{\rho'_{AE}} H_{\min}(A|E)_{\rho'_{AE}}, \quad (\text{A.3})$$

where the supremum ranges over all density operators ρ'_{AE} which are ε -close to ρ_{AE} . Normally, the distance between ρ'_{AE} and ρ_{AE} can be measured by Bures distance $\|\rho - \sigma\|_B = \sqrt{2 - F(\rho, \sigma)}$, where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$ and $\|\cdot\|$ is the l_1 -norm.

Appendix B. Derivation of Eq.(4.3)

With the i.i.d. assumption, the amount of randomness from transmitted quantum states is given by

$$R^{\varepsilon_1}(K_z) = \min_{\rho_{AE}} H_{\min}^{\varepsilon_1}(A|E)_{\Delta_{Z^{\otimes n_z}}^A(\rho_{AE}^{\otimes n_z})}. \quad (\text{B.1})$$

As $n_z \geq \frac{8}{\varepsilon_1} \log_2 \frac{2}{\varepsilon_1}$, the smooth min-entropy can be lower bounded by the conditional von Neumann entropy, $H(A|E)_{\rho_{AE}} = H(\rho_{AE}) - H(\rho_E)$ [29],

$$H_{\min}^{\varepsilon_1}(A|E)_{\Delta_{Z^{\otimes n_z}}^A(\rho_{AE}^{\otimes n_z})} \geq n_z H(A|E)_{\Delta_Z^A(\rho_{AE})} - \sqrt{n_z} \delta(\varepsilon_1, \eta), \quad (\text{B.2})$$

where $\delta(\varepsilon_1, \eta) = 4(\log_2 \eta) \sqrt{\log_2 \frac{2}{\varepsilon_1}}$ and $\eta \leq \sqrt{2^{-H_{\min}(A|E)_{\Delta_Z^A(\rho_{AE})}}} + \sqrt{2^{H_{\max}(A|E)_{\Delta_Z^A(\rho_{AE})}}} + 1$, with H_{\min} and H_{\max} being the min-entropy and maximal-entropy, respectively. Here,

$H_{\min}(A|E)_{\Delta_Z^A(\rho_{AE})} \geq 0$ and $H_{\max}(A|E)_{\Delta_Z^A(\rho_{AE})} \leq 1$ and hence one has $\eta \leq 2 + \sqrt{2}$. Thus $\delta(\varepsilon_1, \eta) \leq k\sqrt{\log_2 \frac{2}{\varepsilon_1^2}}$, with $k = 4\log_2(2 + \sqrt{2}) \approx 7.09$. Therefore, inserting Eq. (B.2) into Eq. (B.1), one has

$$R^{\varepsilon_1}(K_z) \geq n_z \min_{\rho_{AE}} H(A|E)_{\Delta_Z^A(\rho_{AE})} - 7.09\sqrt{n_z \log_2 \frac{2}{\varepsilon_1^2}}. \quad (\text{B.3})$$

Appendix C. Partial derivatives of $C(\rho_A)$

In this section, we analyze the partial derivatives of $C(\rho_A)$. From Eq. (5.3),

$$C(\rho_A) = H(p_z) - H\left(\frac{p_o + 1}{2}\right), \quad (\text{C.1})$$

where $p_o = \sqrt{4(p_x^2 + p_y^2 + p_z^2 - p_x - p_y - p_z) + 3}$. Thus

$$\begin{aligned} \frac{\partial C(\rho_A)}{\partial p_z} &= \frac{\partial}{\partial p_z} \left[H(p_z) - H\left(\frac{p_o + 1}{2}\right) \right] \\ &= \frac{2p_z - 1}{p_o} \log_2 \left(\frac{1 + p_o}{1 - p_o} \right) - \log_2 \left(\frac{p_z}{1 - p_z} \right), \end{aligned} \quad (\text{C.2})$$

$$\frac{\partial C(\rho_A)}{\partial p_x} = \frac{2p_x - 1}{p_o} \log_2 \left(\frac{1 + p_o}{1 - p_o} \right), \quad (\text{C.3})$$

$$\frac{\partial C(\rho_A)}{\partial p_y} = \frac{2p_y - 1}{p_o} \log_2 \left(\frac{1 + p_o}{1 - p_o} \right). \quad (\text{C.4})$$

By analyzing above equations, for $j \in \{x, y, z\}$, $\frac{\partial^2 C(\rho_A)}{\partial p_j^2} \geq 0$. Therefore, function $\frac{\partial C(\rho_A)}{\partial p_j}$ is non-decreasing with p_j . Thus,

$$\begin{aligned} \frac{\partial C(\rho_A)}{\partial p_j} &= 0 & p_j &= 1/2, \\ &\leq 0 & p_j &\leq 1/2, \\ &\geq 0 & p_j &\geq 1/2. \end{aligned}$$

Appendix D. Simulation model

In this section, we analyze a simulation model with a practical experimental setup. Consider a practical source, consisting of a laser and a polarization modulator, which emits N coherent-state pulses with an intensity of μ_0 . We assume the quantum state is prepared to be $|+\rangle$, which is then transmitted through a depolarization channel. Thus, the received quantum state can be described by $\rho_A = p\frac{I}{2} + (1 - p)|+\rangle\langle+|$, where $p \in [0, 1]$. The readout system consists of a polarization rotator (used for basis selection), a polarization beam splitter, and two threshold detectors with the same detection efficiencies. Denote the total transmittance by η , including the detector efficiency and the coupling efficiency between the source and the detector. Here, we

ignore the detection caused by dark counts since for QRNG, dark counts are normally negligible comparing to η .

In the following, we aim to evaluate all the directly obtained experimental statistics. They include the number of total click events, n_j , the number of single-click events of the two detectors, n_j^0 , n_j^1 , and the number of double-click events, n_j^d , when measuring in the $j \in \{X, Y, Z\}$ basis.

Note that the number of photons of the coherent-state pulse follows the Poisson distribution, $P(n) = \frac{e^{-\mu_0} \mu_0^n}{n!}$. With the total transmittance of the system η , the total number of clicks in the X basis is

$$\begin{aligned} n_x &= Nq \sum_n e^{-\mu_0} \frac{\mu_0^n}{n!} [1 - (1 - \eta)^n] \\ &= Nq(1 - e^{-\eta\mu_0}), \end{aligned} \quad (\text{D.1})$$

where q is the probability of selecting the X basis. Similarly, one has

$$n_y = Nq(1 - e^{-\eta\mu_0}), \quad (\text{D.2})$$

$$n_z = N(1 - 2q)(1 - e^{-\eta\mu_0}), \quad (\text{D.3})$$

Denote the probability of double clicks when emitting m photons and measuring in the $j \in \{X, Y, Z\}$ basis by $p_{doub}^{j,m}$. Since the polarization of the input state is $p\frac{1}{2} + (1 - p)|+\rangle\langle+|$, in which only the component $\frac{1}{2}$ may result in the double-click events, then

$$\begin{aligned} p_{doub}^{x,m} &= \frac{p}{2^m} \sum_k C_m^k [1 - (1 - \eta)^k] [1 - (1 - \eta)^{m-k}] \\ &= \frac{p}{2^m} \sum_k [C_m^k - C_m^k (1 - \eta)^k - C_m^k (1 - \eta)^{m-k} + C_m^k (1 - \eta)^m] \\ &= \frac{p}{2^m} [2^m + (1 - \eta)^m 2^m - 2(2 - \eta)^m] \\ &= p(1 + (1 - \eta)^m - 2(1 - \frac{\eta}{2})^m). \end{aligned} \quad (\text{D.4})$$

Meanwhile, for measurement basis Y and Z , both component $\frac{1}{2}$ and $|+\rangle\langle+|$ of ρ_A result in the double-click events with equal probability, thus one has

$$\begin{aligned} p_{doub}^{y,m} &= p_{doub}^{z,m} = \frac{1}{2^m} \sum_k C_m^k [1 - (1 - \eta)^k] [1 - (1 - \eta)^{m-k}] \\ &= 1 + (1 - \eta)^m - 2(1 - \frac{\eta}{2})^m. \end{aligned} \quad (\text{D.5})$$

Thus, the total number of double clicks in the X basis is

$$\begin{aligned} n_x^d &= Nq \sum_m e^{-\mu_0} \frac{\mu_0^m}{m!} p_{doub}^{x,m} \\ &= Nqp(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}). \end{aligned} \quad (\text{D.6})$$

And similarly, one has

$$\begin{aligned} n_y^d &= Nq \sum_m e^{-\mu_0} \frac{\mu_0^m}{m!} p_{doub}^{y,m} \\ &= Nq(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}), \end{aligned} \quad (\text{D.7})$$

$$\begin{aligned}
n_z^d &= N(1-2q) \sum_m e^{-\mu_0} \frac{\mu_0^m}{m!} p_{doub}^{z,m} \\
&= N(1-2q)(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}),
\end{aligned} \tag{D.8}$$

Now we evaluate the number of single-click events corresponding to outcome $|+\rangle$ and $|-\rangle$. Note that, for ρ_A , the component $|+\rangle\langle+|$ never results in outcome $|-\rangle$, while the component $\frac{1}{2}$ contributes to the single-click events of $|+\rangle$ and $|-\rangle$ with the equal probability. Thus one has

$$\begin{aligned}
n_x^0 &= (1-p)n_x + \frac{1}{2}(pn_x - n_x^d) \\
&= Nq(1-p - e^{-\eta\mu_0} + pe^{-\frac{\eta\mu_0}{2}}).
\end{aligned} \tag{D.9}$$

$$\begin{aligned}
n_x^1 &= \frac{1}{2}(pn_x - n_x^d) \\
&= Nqp(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}).
\end{aligned} \tag{D.10}$$

For measurement basis Y and Z , both the component $|+\rangle\langle+|$ and $\frac{1}{2}$ contributes to the single-click events of the two outcomes with the equal probability. Thus one has

$$\begin{aligned}
n_y^0 &= n_y^1 = \frac{1}{2}(n_y - n_y^d) \\
&= Nq(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}).
\end{aligned} \tag{D.11}$$

$$\begin{aligned}
n_z^0 &= n_z^1 = \frac{1}{2}(n_z - n_z^d) \\
&= N(1-2q)(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}).
\end{aligned} \tag{D.12}$$

Combining above results, the experimental obtained statistics are given by

$$n_x^0 = Nq(1-p - e^{-\eta\mu_0} + pe^{-\frac{\eta\mu_0}{2}}), \tag{D.13}$$

$$n_x^1 = Nqp(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}), \tag{D.14}$$

$$n_x^d = Nqp(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}), \tag{D.15}$$

$$n_y^0 = n_y^1 = Nq(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}), \tag{D.16}$$

$$n_y^d = Nq(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}), \tag{D.17}$$

$$n_z^0 = n_z^1 = N(1-2q)(e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}), \tag{D.18}$$

$$n_z^d = N(1-2q)(1 + e^{-\eta\mu_0} - 2e^{-\frac{\eta\mu_0}{2}}), \tag{D.19}$$

$$n_x = Nq(1 - e^{-\eta\mu_0}), \tag{D.20}$$

$$n_y = Nq(1 - e^{-\eta\mu_0}), \tag{D.21}$$

$$n_z = N(1-2q)(1 - e^{-\eta\mu_0}). \tag{D.22}$$

Inserting these expressions into Eq.(5.5), one has

$$\frac{1-p - e^{-\eta\mu_0} + pe^{-\frac{\eta\mu_0}{2}}}{1 - e^{-\eta\mu_0}} \leq p_x \leq \frac{1 - (1-p)e^{-\eta\mu_0} - pe^{-\frac{\eta\mu_0}{2}}}{1 - e^{-\eta\mu_0}}, \tag{D.23}$$

$$\frac{e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}}{1 - e^{-\eta\mu_0}} \leq p_y \leq \frac{1 - e^{-\frac{\eta\mu_0}{2}}}{1 - e^{-\eta\mu_0}}, \tag{D.24}$$

$$\frac{e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}}{1 - e^{-\eta\mu_0}} \leq p_z \leq \frac{1 - e^{-\frac{\eta\mu_0}{2}}}{1 - e^{-\eta\mu_0}}. \tag{D.25}$$

Following the analysis of squashing model and statistical fluctuations, the worst case expectation value of p_x , p_y and p_z are thus given by

$$\bar{p}_x = P_x^L - \theta = \frac{1 - p - e^{-\eta\mu_0} + pe^{-\frac{\eta\mu_0}{2}}}{1 - e^{-\eta\mu_0}} - \theta, \quad (\text{D.26})$$

$$\bar{p}_y = P_y^L - \theta = \frac{e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}}{1 - e^{-\eta\mu_0}} - \theta, \quad (\text{D.27})$$

$$\bar{p}_z = P_z^L - \theta = \frac{e^{-\frac{\eta\mu_0}{2}} - e^{-\eta\mu_0}}{1 - e^{-\eta\mu_0}} - \theta. \quad (\text{D.28})$$

Inserting \bar{p}_j into Eq. (5.8) or (5.12), one can estimate the amount of extractable randomness from the raw random bits.

References

- [1] Born M 1926 *Zeitschrift für Physik* **37** 863–867
- [2] Ma X, Yuan X, Cao Z, Qi B and Zhang Z 2016 *npj Quantum Information* **2** 16021 review Article URL <http://dx.doi.org/10.1038/npjqi.2016.21>
- [3] Herrero-Collantes M and Garcia-Escartin J C 2016 *arXiv preprint arXiv:1604.03304*
- [4] Peter B The nsas work to make crypto worse and better <https://arstechnica.com/security/2013/09/the-nsas-work-to-make-crypto-worse-and-better/>
- [5] Ma X, Xu F, Xu H, Tan X, Qi B and Lo H K 2013 *Phys. Rev. A* **87**(6) 062327 URL <http://link.aps.org/doi/10.1103/PhysRevA.87.062327>
- [6] Pironio S, Acín A, Massar S, de La Giroday A B, Matsukevich D N, Maunz P, Olmschenk S, Hayes D, Luo L, Manning T A *et al.* 2010 *Nature* **464** 1021–1024
- [7] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 *Reviews of Modern Physics* **86** 419
- [8] Miller C A and Shi Y 2014 *arXiv preprint arXiv:1411.6608*
- [9] Arnon-Friedman R, Renner R and Vidick T 2016 *arXiv preprint arXiv:1607.01797*
- [10] Cao Z, Zhou H and Ma X 2015 *New Journal of Physics* **17** 125011
- [11] Cao Z, Zhou H, Yuan X and Ma X 2016 *Physical Review X* **6** 011020
- [12] Marangon D G, Vallone G and Villoresi P 2017 *Phys. Rev. Lett.* **118**(6) 060503 URL <http://link.aps.org/doi/10.1103/PhysRevLett.118.060503>
- [13] Bischof F, Kampermann H and Bruß D 2017 *ArXiv e-prints (Preprint 1703.03330)*
- [14] Yuan X, Zhou H, Cao Z and Ma X 2015 *Phys. Rev. A* **92**(2) 022124 URL <http://link.aps.org/doi/10.1103/PhysRevA.92.022124>
- [15] Yuan X, Zhao Q, Girolami D and Ma X 2016 *arXiv preprint arXiv:1605.07818*
- [16] Baumgratz T, Cramer M and Plenio M B 2014 *Phys. Rev. Lett.* **113**(14) 140401 URL <http://link.aps.org/doi/10.1103/PhysRevLett.113.140401>
- [17] Napoli C, Bromley T R, Cianciaruso M, Piani M, Johnston N and Adesso G 2016 *Physical review letters* **116** 150502
- [18] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
- [19] Ma X, Fung C H F and Lo H K 2007 *Phys. Rev. A* **76**(1) 012307 URL <http://link.aps.org/doi/10.1103/PhysRevA.76.012307>
- [20] Beaudry N J, Moroder T and Lütkenhaus N 2008 *Physical review letters* **101** 093601
- [21] Fung C H F, Chau H and Lo H K 2011 *Physical Review A* **84** 020303
- [22] Shor P W and Preskill J 2000 *Physical review letters* **85** 441
- [23] Eisert J, Brandão F G and Audenaert K M 2007 *New Journal of Physics* **9** 46
- [24] Gühne O, Reimpell M and Werner R 2007 *Physical review letters* **98** 110502
- [25] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 *Nature Physics* **6** 659–662

- [26] König R, Renner R and Schaffner C 2009 *IEEE Transactions on Information theory* **55** 4337–4347
- [27] Impagliazzo R, Levin L A and Luby M 1989 Pseudo-random generation from one-way functions *Proceedings of the twenty-first annual ACM symposium on Theory of computing* (ACM) pp 12–24
- [28] Christandl M, König R and Renner R 2009 *Physical review letters* **102** 020504
- [29] Tomamichel M, Colbeck R and Renner R 2009 *IEEE Transactions on Information Theory* **55** 5840–5847
- [30] Hoeffding W 1963 *Journal of the American statistical association* **58** 13–30
- [31] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72**(1) 012326 URL <http://link.aps.org/doi/10.1103/PhysRevA.72.012326>
- [32] Fung C H F, Ma X and Chau H F 2010 *Phys. Rev. A* **81**(1) 012318 URL <http://link.aps.org/doi/10.1103/PhysRevA.81.012318>
- [33] Zhou H, Yuan X and Ma X 2015 *Phys. Rev. A* **91**(6) 062316 URL <https://link.aps.org/doi/10.1103/PhysRevA.91.062316>